62788-043
Kunihiko MIYAZAKI
et al.

日 本 国 特 許 庁
JAPAN PATENT OFFICE

July 17, 2003
McDermott, Will & Emery

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年　７月１７日

出願番号
Application Number: 特願２００２－２０７６９６

[ST.10/C]: [ＪＰ２００２－２０７６９６]

出願人
Applicant(s): 株式会社日立製作所

２００３年　６月１９日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３０４８００５

【書類名】　特許願

【整理番号】　K02009781A

【あて先】　特許庁長官殿

【国際特許分類】　G09C　1/00

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

【氏名】　宮崎　邦彦

【発明者】

【住所又は居所】　東京都江東区新砂一丁目６番２７号　株式会社日立製作所公共システム事業部内

【氏名】　大本　周広

【特許出願人】

【識別番号】　000005108

【氏名又は名称】　株式会社　日立製作所

【代理人】

【識別番号】　100075096

【弁理士】

【氏名又は名称】　作田　康夫

【手数料の表示】

【予納台帳番号】　013088

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【その他】　国等の委託研究の成果に係る特許出願（平成１４年度通信・放送機構「次世代証拠基盤技術に関する研究開発」委託研究、産業活力再生特別措置法第３０条の適用を受

けるもの）

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　ディジタル署名の検証方法

【特許請求の範囲】

【請求項１】

メッセージに対するディジタル署名を検証するディジタル署名の検証方法であって、

ディジタル署名生成者側の装置において、

メッセージあるいはそのハッシュ値に、ディジタル署名生成者が所有する秘密鍵を作用させ、当該メッセージに対するディジタル署名を生成する署名生成ステップと、

生成したディジタル署名とメッセージとを含むディジタル署名付きメッセージを配布するとともに、当該ディジタル署名付きメッセージのログデータをログリストに登録する登録ステップと、を有し、

ディジタル署名検証者側の装置において、

配布されたディジタル署名付きメッセージを、検証対象ディジタル署名付きメッセージとして受け付ける検証対象受付ステップと、

前記検証対象ディジタル署名付きメッセージを配布したディジタル署名者のログリストを取得する履歴取得ステップと、

前記検証対象ディジタル署名付きメッセージのログデータが、前記ログリストに登録されているか否かを調べる履歴有無検証ステップとを備え、

登録されている場合は、さらに、前記ログリストに含まれるログデータの信頼度を設定する個別信頼度設定ステップと、

設定された個別信頼度から前記ログリストの信頼度を算出する履歴信頼度算出ステップと、

当該検証対象ディジタル署名付きメッセージが前記ディジタル署名生成者側装置により配布されたものであることを、信頼度付きで認証する検証ステップと、

を有することを特徴とするディジタル署名の検証方法。

【請求項２】

メッセージに対するディジタル署名に関する係争を解決する調停方法であって

調停において、

調停依頼者装置から調停対象となるディジタル署名付きメッセージを受け付ける要求受付ステップと、

前記調停対象となるディジタル署名付きメッセージに関するログリストを入手する履歴入手ステップと、

請求項１記載の検証ステップと、

前記検証ステップの出力である信頼度に基づき、調停結果を出力する調停ステップと、

を有することを特徴とする調停方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は情報セキュリティに関する。

【０００２】

【従来の技術】

電子署名の安全性を高める技術として、署名生成時にその記録を履歴として残しておき、また、新たに署名を生成する際には、その時点における履歴データを反映させることにより、署名間に論理的な連鎖関係を構築する技術（これをヒステリシス署名と呼ぶ）がある。

【０００３】

上記ヒステリシス署名技術については、特開2001-331104号公報などに開示されている。

【０００４】

【発明が解決しようとする課題】

上記ヒステリシス署名技術では、署名の検証を行う際に、当該に関する署名履歴を利用している。したがって、この署名履歴の信頼度を適切に反映するように構成されたヒステリシス署名の検証方法が望まれている。

【０００５】

【課題を解決するための手段】

本発明は、署名履歴の信頼度を適切に反映するように構成されたヒステリシス署名の検証方法を提供する。

【０００６】

本発明の一態様によれば、ヒステリシス署名検証において、検証に利用される署名生成履歴（ログリストという）に含まれる各署名生成記録（ログデータという）に対し個別信頼度を設定し、個別信頼度から署名生成履歴の信頼度を算出し、これを検証結果の信頼度として出力する、ヒステリシス署名の検証方法を提供する。

【０００７】

また本発明の一態様によれば、ある署名の真偽をめぐって二者（あるいはそれ以上）の間で係争が起こったときに、上記ヒステリシス署名の検証方法にしたがって出力された検証結果の信頼度に基づき、調停結果を出力する調停方法を提供する。

【０００８】

【発明の実施の形態】

図１は、本発明の第１実施形態が適用されたシステムの概略図である。

【０００９】

図示するように、ネットワーク5を介して、ヒステリシス署名を生成する署名者が利用する装置である署名者装置1と、前記署名者装置1において生成された署名生成履歴を管理する履歴管理装置2と、前記署名者が生成した署名の正当性に関し調停を依頼する調停依頼者が利用する調停依頼者装置3と、依頼に応じて署名の正当性判定を行い調停する調停者装置4とが接続されている。なお図１には、それぞれの装置が一台ずつ存在する場合を示しているが、一般には複数存在していてよい。

【００１０】

図２は、署名者装置1の概略構成を示した図である。

【００１１】

署名者装置1は、CPU11と、CPU11のワークエリアとして機能するRAM12と、ハー

ドディスク装置などの外部記憶装置13と、CD-ROMやFDなどの可搬性を有する記憶媒体15からデータを読取る読取り装置14と、キーボードやマウスなどの入力装置16と、ディスプレイなどの表示装置17と、ネットワークを介して他の装置と通信を行うための通信装置18と、上述した各構成要素間のデータ送受を司るインターフェイス20を備えた、一般的な構成を有する電子計算機21で構築することができる。

【００１２】

署名者装置1の外部記憶装置13に格納されるのは、メッセージに対するディジタル署名を生成し、生成されたディジタル署名（ヒステリシス署名）を付したヒステリシス署名付きメッセージを配布し、また、履歴管理装置2に対し署名生成記録の登録を依頼するための、署名付きメッセージ作成PG（プログラム）131である。これは、RAM12上にロードされ，CPU11により、署名付きメッセージ作成処理部111というプロセスとして具現化される。

【００１３】

履歴管理装置2、調停依頼者装置3、調停者装置4も署名者装置1と同様の構成を備える。

【００１４】

履歴管理装置2の外部記憶装置13に格納されるのは、署名者装置1から登録を依頼された署名生成記録を受信し、当該署名生成記録を署名履歴として登録する履歴登録PG（プログラム）132と、署名者装置1や、調停依頼者装置3や、調停者装置4からの要求に応じて、自履歴管理装置2が管理する署名履歴を送信する履歴送信PG（プログラム）133である。これらは、RAM12上にロードされ、CPU11により履歴登録処理部112や履歴送信処理部113というプロセスとして具現化される。

【００１５】

調停依頼者装置3の外部記憶装置13に格納されるのは、調停対象となるヒステリシス署名付きメッセージに関する署名履歴を履歴管理装置2に要求し受信する履歴要求PG（プログラム）134と、調停対象となるヒステリシス署名付きメッセージとそれに関する署名履歴を調停者装置4に送信し、調停を依頼する調停依頼PG（プログラム）135である。これは、RAM12上にロードされ、CPU11により履歴要

求処理部114や調停依頼処理部115というプロセスとして具現化される。

【００１６】

調停者装置4の外部記憶装置13に格納されるのは、各調停依頼者装置3からヒステリシス署名付きメッセージとそれに関する署名履歴を受信し、最も信頼度の高い調停依頼者を判定する調停PG（プログラム）136である。これらは、RAM12上にロードされ、CPU11により調停処理部116というプロセスとして具現化される。

【００１７】

各プログラムは、予め外部記憶装置13に格納されていても良いし、必要に応じて、読取り装置14を介して記憶媒体15から、または通信装置18とネットワークを介して、他の装置から導入されても良い。

【００１８】

本実施例においては、署名者装置1、履歴管理装置2、調停依頼者装置3、調停者装置4を、それぞれ独立した装置としているが、これと異なっていてもよい。たとえば、署名者装置1の機能と履歴管理装置2の機能が同一装置上で実現されていてもよい。この場合、署名者の署名生成記録を署名者自身によって管理できるため、履歴管理装置2に対し署名生成記録の登録を依頼する必要がなくなる。

【００１９】

あるいは、履歴管理装置2の機能と調停者装置3の機能を同一装置上に実現してもよい。この場合、調停依頼者が調停者装置3に対し、調停を依頼するときに、事前に調停対象となるヒステリシス署名付きメッセージに関する署名履歴を入手する必要がなくなるため、効率的である。また、通常、取引の際には、双方向でデータがやり取りされることを考えると、同一人が、ある場面においては署名者であり、別の場面においては調停依頼者となることも考えられる。このような場合には、署名者装置1の機能と調停依頼者装置3の機能を同一装置上に実現すればよい。

【００２０】

なお、本実施例においては、署名者装置1が複数台存在する場合には、履歴管理装置2は、それら複数の署名者装置1の署名生成記録を管理するようにしてもよい。

【００２１】

図３は、署名者装置1の署名付きメッセージ作成PG131の処理フローを示す。

ステップ３０１：はじめ。

ステップ３０２：署名対象メッセージを作成する。

ステップ３０３：署名対象メッセージに対しヒステリシス署名を生成する。

ステップ３０４：ステップ３０３で生成された署名に関する署名生成記録（ログデータ）を履歴管理装置2に送る（登録を依頼する）。

ステップ３０５：（必要であれば）ヒステリシス署名付きメッセージを公開鍵証明書をつけて受信者装置に送る。

ステップ３０６：おわり。

【００２２】

なお、ステップ３０５における受信者装置は、図１には図示されていない。たとえば、署名対象メッセージが、取引契約書である場合、当該契約書の受け取り手である取引相手の装置がこれに該当する。受信者装置の概略構成は、図２と同様でよい。また、調停依頼者が受信者となり、調停依頼者装置と受信者装置とが同じであっても良い。

【００２３】

また、ステップ３０３におけるヒステリシス署名の生成は、具体的には以下に示す「ヒステリシス署名生成処理」の手順に従って実現可能である。なお説明にあたっては、以下の記法を用いる。また、署名者をAliceと称することにする。

【００２４】

「記法」

Sign_K() ： 署名生成鍵Kを用いた、従来の電子署名方式(例：RSA署名、DSA署名、ECDSA署名など)における署名生成処理

Verify_K() ： 署名検査鍵Kを用いた、従来の電子署名方式における署名検査処理

h() ： 一方向性ハッシュ関数(例：SHA-1ハッシュ関数、MD5ハッシュ関数など)

A||B ： 二つのデータA,Bを連結したデータ

Ks ： Aliceの署名生成鍵

Kv ： Aliceの署名検査鍵

n ： Aliceがヒステリシス署名生成を行った回数

IV ： 初期値

Mn ： n 番目の署名対象メッセージ

Sn ： n 番目のヒステリシス署名付きメッセージ

Rn ： n 番目のヒステリシス署名生成記録

Hn ： n 回目のヒステリシス署名生成を行った後の署名生成履歴（1 回目からn 回目までのヒステリシス署名生成記録を連結したデータ。

【００２５】

「ヒステリシス署名生成処理」

ステップ３０３１：（署名生成フェーズ）署名対象メッセージMnのハッシュ値h(Mn)を算出する。

ステップ３０３２：保存してある署名生成履歴Hn-1に含まれる最新の署名生成記録Rn-1のハッシュ値h(Rn-1)を算出する。ただし，1回目のヒステリシス署名生成処理においては，以降の手順でハッシュ値h(Rn-1)の代わりに初期値IVを用いる。

ステップ３０３３：ステップ３０３１、３０３２で算出した二つのハッシュ値を連結したデータh(Mn)||h(Rn-1)に対して，署名生成鍵Ksを用いて従来の署名生成処理を行い，電子署名付きメッセージSign_Ks(h(Mn)||h(Rn-1))を生成する。

ステップ３０３４：署名対象メッセージMn，最新の署名生成記録のハッシュ値h(Rn-1)，および電子署名付きメッセージSign_Ks(h(Mn)||h(Rn-1))を連結し，ヒステリシス署名付きメッセージSn=Mn||h(Rn-1)||Sign_Ks(h(Mn)||h(Rn-1))を生成する。

ステップ３０３５：（署名生成履歴更新フェーズ）二つのハッシュ値h(Mn)，h(Rn-1)と電子署名付きメッセージSign_Ks (h(Mn)||h(Rn-1))とを連結し，署名生成記録

Rn=h(Mn)||h(Rn-1)||Sign_Ks(h(Mn)||h(Rn-1))を生成する。

ステップ３０３６：保存してある署名生成履歴Hn-1と署名生成記録Rnとを連結し，署名生成履歴Hn=Hn-1||Rnを生成して保存する。

【００２６】

なお上記ステップ３０３１では、署名対象メッセージMnのハッシュ値h(Mn)を算出しているが、署名生成処理Sign_K()が許容するのであれば、以降の処理で、ハッシュ値のかわりに、署名対象メッセージMnそのものを用いてもよい。署名生成処理Sign_K()が許容する例としては、たとえば、入力データ長にあわせて署名生成処理Sign_K()を繰り返し適用することにより任意長のデータを許容可能とする方法などがある。

【００２７】

図４は、履歴管理装置2の履歴登録PG132の処理フローを示す。

ステップ４０１：はじめ。

ステップ４０２：署名者装置1から署名生成記録を受信する（登録依頼を受け付ける）。(署名者をAliceとする)

ステップ４０３：すでに登録済みのAliceの署名生成履歴（ログリスト）との整合性をチェックし整合していればステップ４０５へ。そうでなければ４０４へ。

ステップ４０４：「登録失敗」という結果を署名者装置1に返し、おわり。

ステップ４０５：ステップ４０２で受け付けた署名生成記録をAliceの署名生成履歴に追記する。

ステップ４０６：「登録成功」という結果を署名者装置1に返す。

ステップ４０７：おわり。

【００２８】

なお、ステップ４０３における整合性のチェックは、具体的には以下のようにして実現可能である。なお、ステップ４０２で受信した署名生成記録Hnとし、ステップ４０３の時点ですでに登録済みのAliceの署名生成履歴をHn-1とする。

【００２９】

まず、署名生成履歴をHn-1のなかの最新の署名生成記録Hn-1のハッシュ値h(Hn-1)を算出する。次に、算出したハッシュ値h(Hn-1)が、ステップ４０２で受信した署名生成記録Hnの中のハッシュ値h(Hn-1)と一致するか否かを確認する。一致すれば、整合していると判定し、そうでなければ整合していないと判定する。

【００３０】

図５は、履歴管理装置3の履歴送信PG133の処理フローを示す。

ステップ５０１：はじめ。

ステップ５０２：履歴送信要求（署名者名、要求履歴範囲(何番目から何番目までか)などを含む）を受け付ける。

ステップ５０３：要求を受け付けた範囲の署名生成記録からなる署名生成履歴を要求者に送信する。

ステップ５０４：おわり。

【００３１】

図６は、調停依頼者装置3の履歴要求PG134の処理フローを示す。

ステップ６０１：はじめ。

ステップ６０２：調停依頼対象となるヒステリシス署名付きメッセージに関する署名生成履歴の送信を、履歴管理装置2に要求する。（当該ヒステリシス署名の署名者名、要求範囲（例：当該ヒステリシス署名に関する署名生成記録から、現時点での最新の署名生成記録までの全ての署名生成記録からなる署名生成履歴）を送る。）

ステップ６０３：履歴管理装置2から、署名生成履歴を受信する。

ステップ６０４：おわり。

【００３２】

図７は、調停依頼者装置3の調停依頼PG135の処理フローを示す。

ステップ７０１：はじめ。

ステップ７０２：調停者装置4に対し、調停依頼対象となるヒステリシス署名付きメッセージと、履歴管理装置2から入手した、当該ヒステリシス署名付きメッセージに関する署名生成記録を含む署名生成履歴を送信し、調停を依頼する。

ステップ７０３：調停結果を受信する。

ステップ７０４：おわり。

【００３３】

図８は、調停者装置4の調停PG136の処理フローを示す。

ステップ８０１：はじめ。

ステップ８０２：ヒステリシス署名付きメッセージに関する係争を行っている調停依頼者が使用する調停依頼者装置3（一般には複数）から調停要求を受け付け

る。

ステップ８０３：それぞれの調停依頼者装置3から受け付けたヒステリシス署名付きメッセージと署名生成履歴を信頼度付きで検証する。ステップ８０４：もっとも高い信頼度となったヒステリシス署名付きメッセージを提出した調停依頼者の名前を、調停結果として出力する。（調停依頼者装置3達に送信する）

ステップ８０５：おわり。

【００３４】

なお、上記ステップ８０３における検証処理は、具体的には以下に示す「ヒステリシス署名検証処理」の手順に従って実現可能である。

【００３５】

「ヒステリシス署名検証処理」

まず、ヒステリシス署名付きメッセージSnの検証を、次のように行う。

ステップ８０３１：ヒステリシス署名付きメッセージSnに含まれる署名対象メッセージMnのハッシュ値h(Mn)を算出する。

ステップ８０３２：ステップ８０３１で算出したハッシュ値h(Mn)と、ヒステリシス署名付きメッセージSnに含まれるハッシュ値h(Rn-1)および電子署名付きメッセージSignKs(h(Mn)||h(Rn-1))と、Alice の公開鍵証明書に含まれる署名検査鍵Kvとを用いて従来の署名検証処理を行う。検証できなければ検証失敗として終了。

ステップ８０３３：Aliceの署名生成履歴Hnのなかに、検証対象となっているヒステリシス署名付きメッセージに対応する署名生成記録

Rm=h(Mm)||h(Rm-1)||SignKs(h(Mn)||h(Rm-1))

が含まれていることを確認する。確認できなければ、検証失敗として終了。

ステップ８０３４：k=mとし、以下の署名生成履歴Hnの整合性検証を行う。

（i）署名生成履歴Hnに含まれる署名生成記録Rk-1のハッシュ値h(Rk-1) を算出する。

（ii）署名生成記録Rkの中のハッシュ値h(Rk-1)が、上で算出したh(Rk-1)と同じ値であることを確認する。確認できなければ、ステップ８０３５へ。

（iii）k<nであれば、k:=k+1とし、（i）へ。そうでなければ、ステップ８０３

５へ。

ステップ８０３５：署名生成履歴Hnのうち整合性が確認できた署名生成記録Rm,...,Rkについて、それぞれの信頼度を設定する。

ステップ８０３６：ステップ８０３５で設定された各署名生成記録の信頼度から、検証対象となる署名に対応する署名生成記録Rmの信頼度を算出し、これを検証結果（「検証成功」）の信頼度として出力する。

【００３６】

なお、上記のステップ８０３５で設定する署名生成記録の信頼度は、たとえば、次に述べる個別信頼度とすればよい。

【００３７】

署名生成記録Ri の個別信頼度とは，Ri の検査手順によって決まる値

f_rely(Ri) = (pind(Ri), qind(Ri), tind(Ri))

のことである。ただし，pind(Ri)，qind(Ri)，tind(Ri) は，他の署名生成記録とは独立に，以下で定義される。

pind(Ri)：Ri が正当であるとき，当該検査手順によって「正当」と判定される確率(1/2 <= pind(Ri) <= 1)

qind(Ri)：Ri が偽造であるとき，当該検査手順によって「正当」と判定される確率(0 <= qind(Ri) <= 1/2)

tind(Ri)：当該検査手順によるRi の判定結果(Ri が「正当」と判定されたときtind(Ri) = 1，Ri が「偽造」と判定されたときtind(Ri) = 0)

なお、判断材料がない等の理由により、ある署名生成記録Ri の検査ができない場合には、個別信頼度は、

f_rely(Ri) =(1/2, 1/2, 1) と設定するものとする。

【００３８】

また、上記のステップ８０３６で算出する検証対象となる署名に対応する署名生成記録Rmの信頼度とは、たとえば次にのべる署名生成履歴の信頼度とすればよい。

【００３９】

署名生成履歴Hn の署名生成記録Rm に関する信頼度とは、Rm が実際に正当で

ある確率f_post_rely(Rm) のことである。f_post_rely(Rm)については、次の命題が成り立つ。

【００４０】

（命題１）

f_post_rely(Rm)

>= Π_{i=m,,,k} Pind(Ri)

/ (Π_{i=m,,,k} Pind(Ri)

+ Π_{i=m,,,k} Qind(Ri))… (式１)

（ただし、Π_{i=m,,,k} Xi は、XmからXkまでの総積をあらわす。すなわち、Π_{i=m,,,k} Xi = Xm×…×Xkである。

Pind(Ri)は、tind(Ri)=1の時はpind(Ri)、

tind(Ri)=0の時は1-pind(Ri)で、

Qind(Ri)は、tind(Ri)=1の時はqind(Ri)、

tind(Ri)=0の時は1-qind(Ri)とする。）

が成り立つ。

【００４１】

（証明の概略）今、署名生成記録Ri とRi+1 が連鎖しているとし、それぞれ適切な検査手順によって正当であると判定されたとする。すなわち、

f_rely(Rj) = (pind(Rj), qind(Rj), 1) (j =i, i+1) であったとする。このとき、Ri+1が実際に正当である確率を、f_post_rely(Ri+1) と書くと、他に条件がなければ、

f_post_rely(Ri+1)

= pind(Ri+1)/(pind(Ri+1)+qind(Ri+1)) である。

【００４２】

一方、Ri が実際に正当である確率を考える。Ri はRi+1 と連鎖しており、また、Ri+1 が実際に正当である確率が分かっている。ハッシュ関数の一方向性から、Ri が実際に正当であることの事前確率f_pri_rely(Ri) は、

f_pri_rely(Ri) >= f_post_rely(Ri+1) を満たす。したがって、Ri が実際に正当である確率f_post_rely(Ri)は、

```
f_post_rely(Ri)
= f_pri_rely(Ri) pind(Ri)
  / (f_pri_rely(Ri) pind(Ri)
    + (1 - f_pri_rely(Ri)) qind(Ri))
>= f_post_rely(Ri+1) pind(Ri)
  / (f_post_rely(Ri+1) pind(Ri)
   + (1 - f_post_rely(Ri+1)) qind(Ri))
= pind(Ri+1) pind(Ri)
  / (pind(Ri+1) pind(Ri) + qind(Ri+1) qind(Ri))
```

となる。これを繰り返し適用すればよい。（証明終わり）

命題１より、署名生成記録Rmの信頼度は、上記（式１）の右辺の値で下から評価できることが分かる。したがって、たとえば、上記のステップ８０３６で算出する検証対象となる署名に対応する署名生成記録Rmの信頼度を、上記（式１）の右辺の値とすれば、署名の検証結果を適切に評価することが可能となる。

【００４３】

本実施例に述べた信頼度付きヒステリシス署名検証方法に従えば、署名履歴の信頼度を適切に判定した検証方法が実現可能となる。また、この検証方法に基づいて判定を行うことにより、ヒステリシス署名付きメッセージをめぐる係争を解決する調停方法および調停者装置を提供可能となる。

【００４４】

【発明の効果】

本発明によれば、署名履歴の信頼度を適切に反映するように構成された検証方法を提供することが可能となる。また、この検証方法に基づいて署名の正当性をめぐる係争を解決する調停方法および調停者装置が提供可能となる。

【図面の簡単な説明】

【図１】本発明の第１実施形態が適用されたシステムの概略図である。

【図２】署名者装置1、履歴管理装置2、調停依頼者装置3、調停者装置4の概略構成を示した図である。

【図３】署名者装置の署名付きメッセージ作成PG131の処理フローを示す。

【図４】履歴管理装置の履歴登録PG132の処理フローを示す。

【図５】履歴管理装置の履歴送信PG133の処理フローを示す。

【図６】調停依頼者装置の履歴要求PG134の処理フローを示す。

【図７】調停依頼者装置の調停依頼PG135の処理フローを示す。

【図８】調停者装置の調停PG136の処理フローを示す。

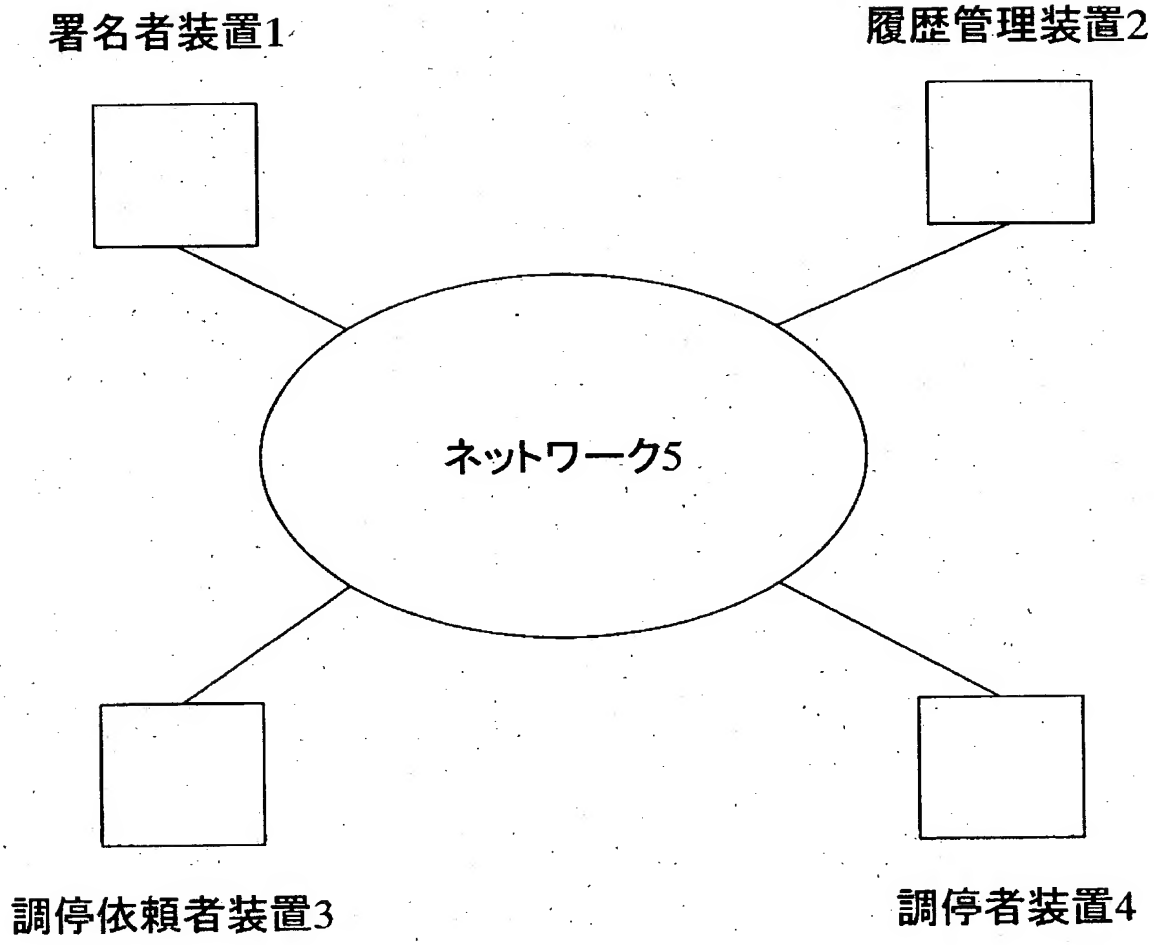
【符号の説明】

1…署名者装置、2…履歴管理装置、3…調停依頼者装置、4…調停者装置、11…CPU、12…RAM、13…外部記憶装置、14…読取装置、15…可搬性記憶媒体、16…入力装置、17…表示装置、18…通信装置、20…インターフェイス、21…電子計算機、131…署名付きメッセージ作成PG、132…履歴登録プログラム、133…履歴送信プログラム、134…履歴要求プログラム、135…調停依頼プログラム、136…調停プログラム。

【書類名】　図面

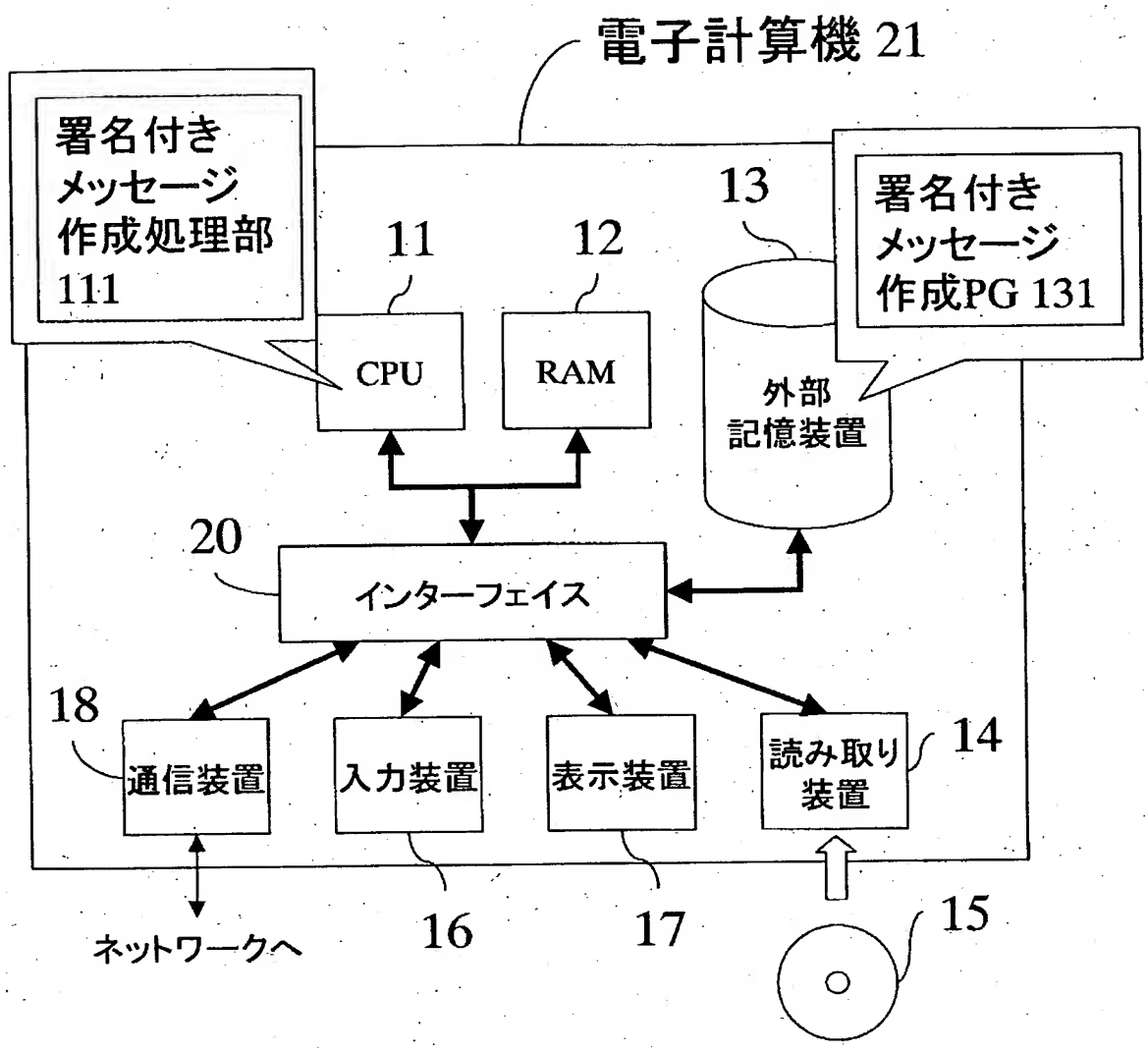
【図１】

図１



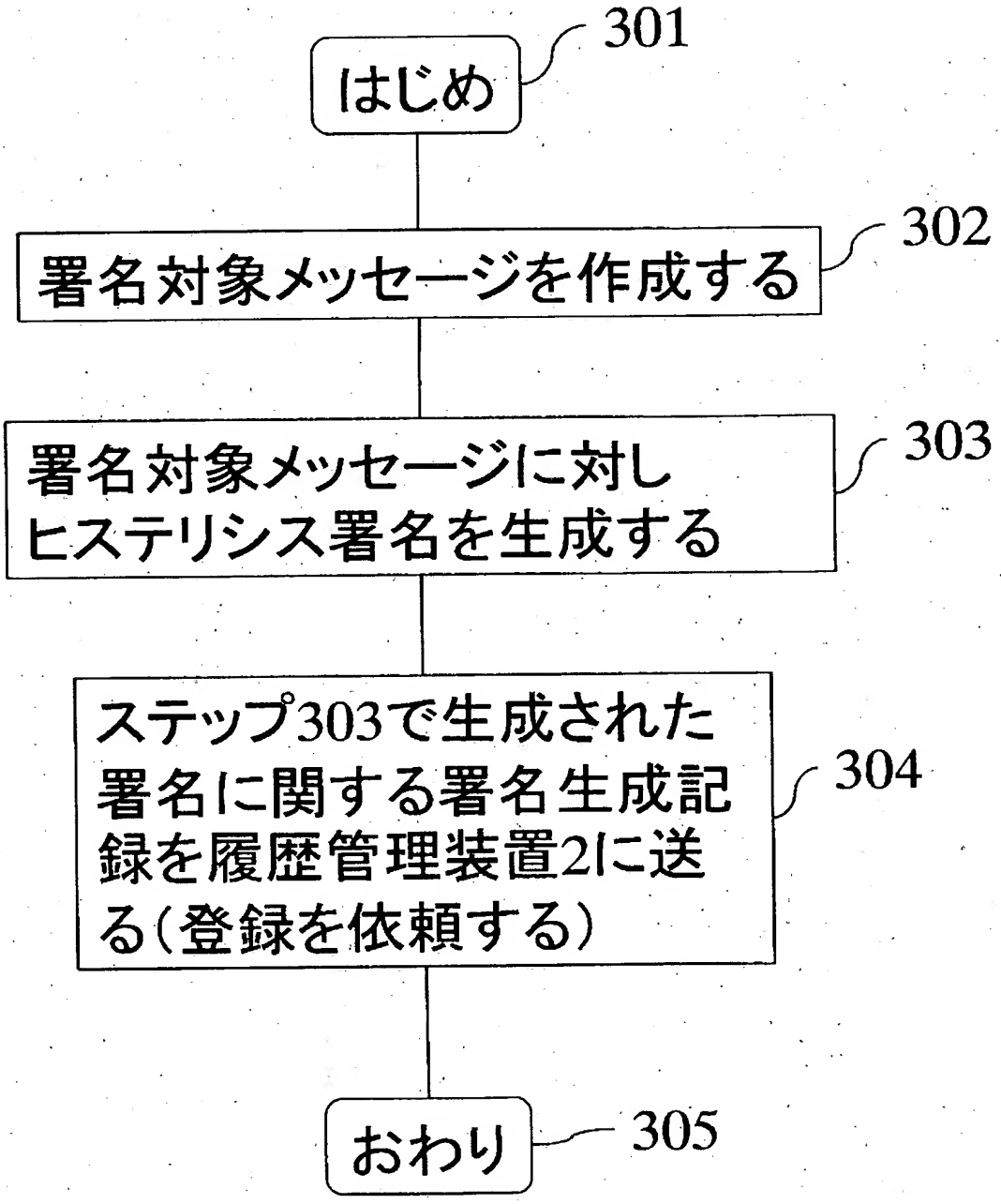
【図２】

図2


電子計算機 21
署名付き
メッセージ
作成処理部
111
11
12
13
署名付き
メッセージ
作成PG 131
CPU
RAM
外部
記憶装置
20
インターフェイス
18
通信装置
入力装置
表示装置
読み取り
装置
14
ネットワークへ
16
17
15

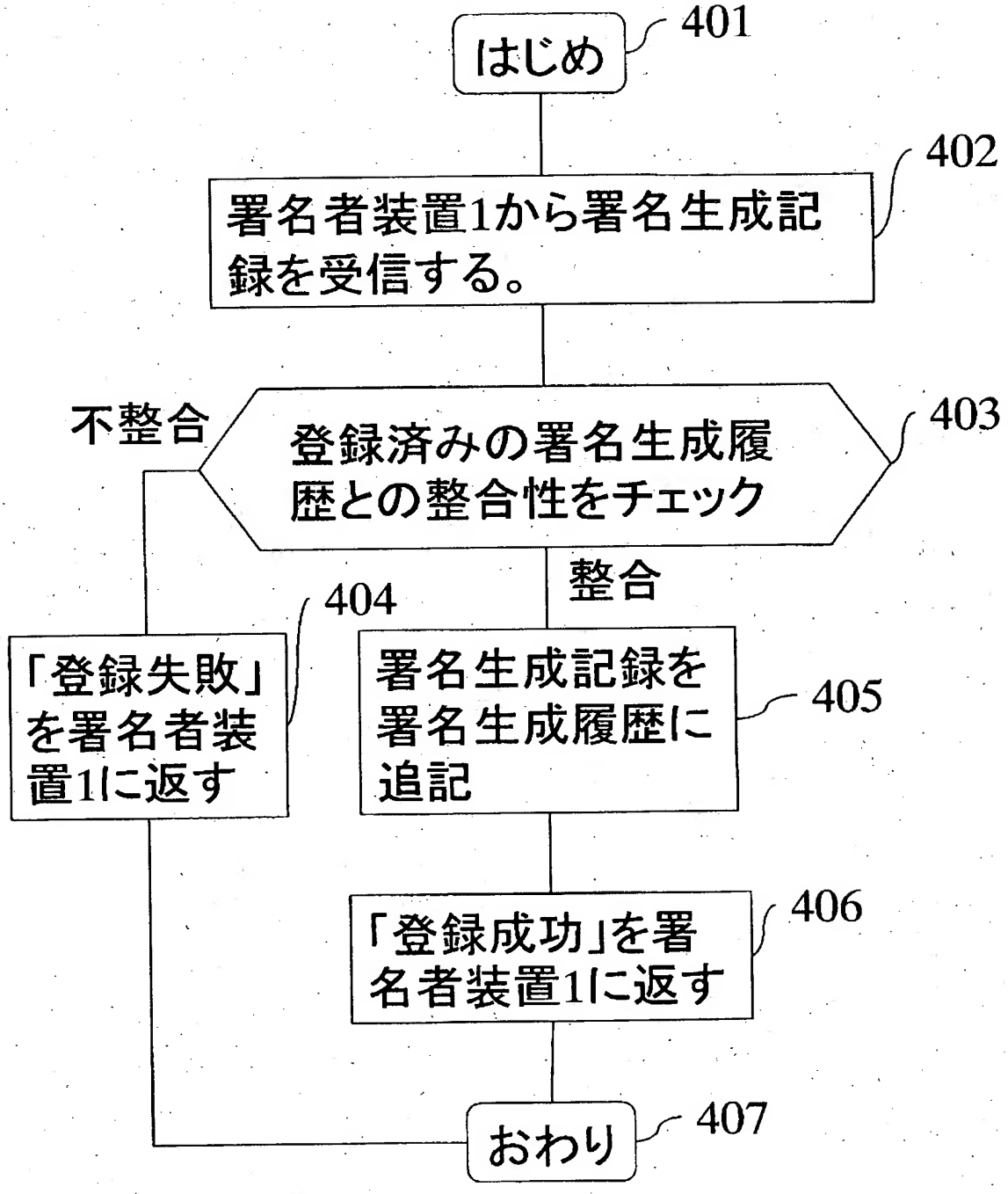
【図３】

図3


はじめ
301
署名対象メッセージを作成する
302
署名対象メッセージに対し
ヒステリシス署名を生成する
303
ステップ303で生成された
署名に関する署名生成記
録を履歴管理装置2に送
る（登録を依頼する）
304
おわり
305

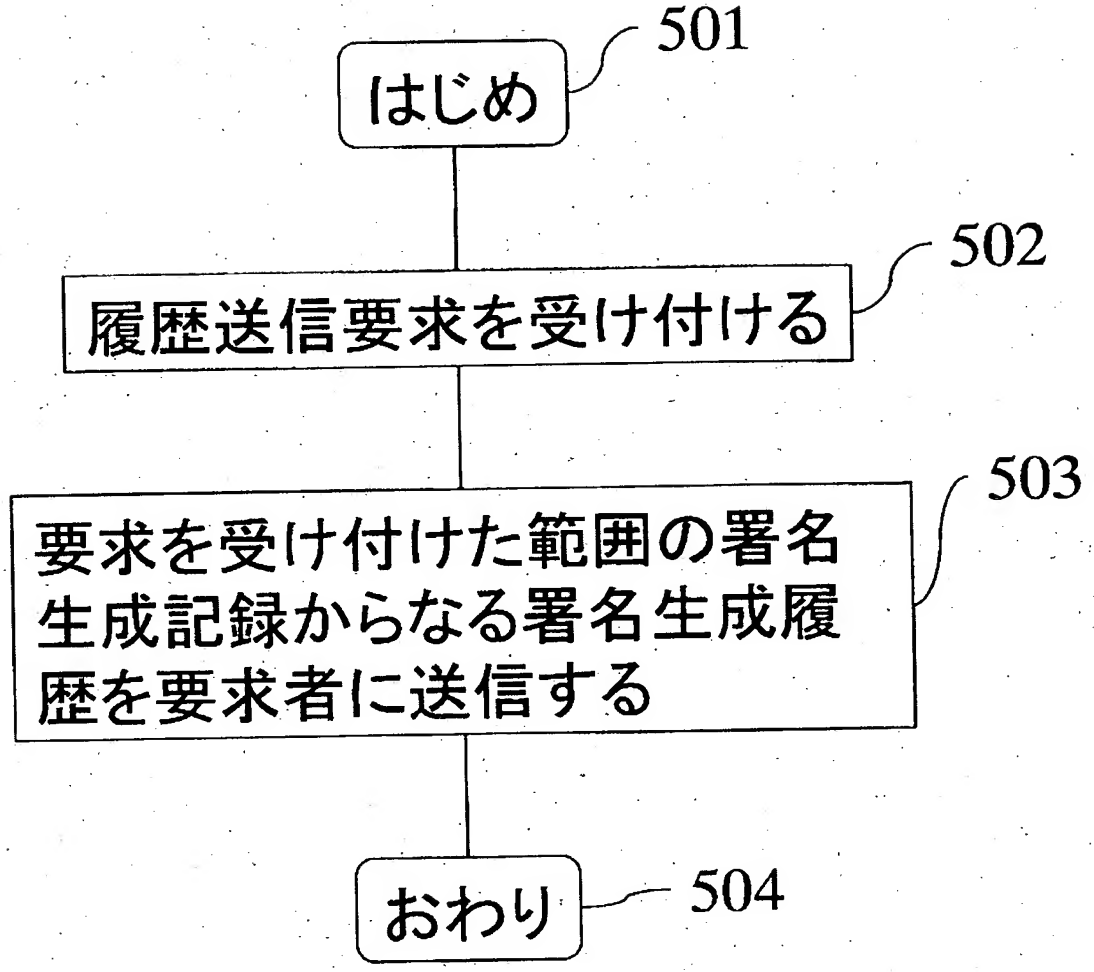
【図４】

図4


はじめ
401
署名者装置1から署名生成記録を受信する。
402
登録済みの署名生成履歴との整合性をチェック
403
不整合
整合
「登録失敗」を署名者装置1に返す
404
署名生成記録を署名生成履歴に追記
405
「登録成功」を署名者装置1に返す
406
おわり
407

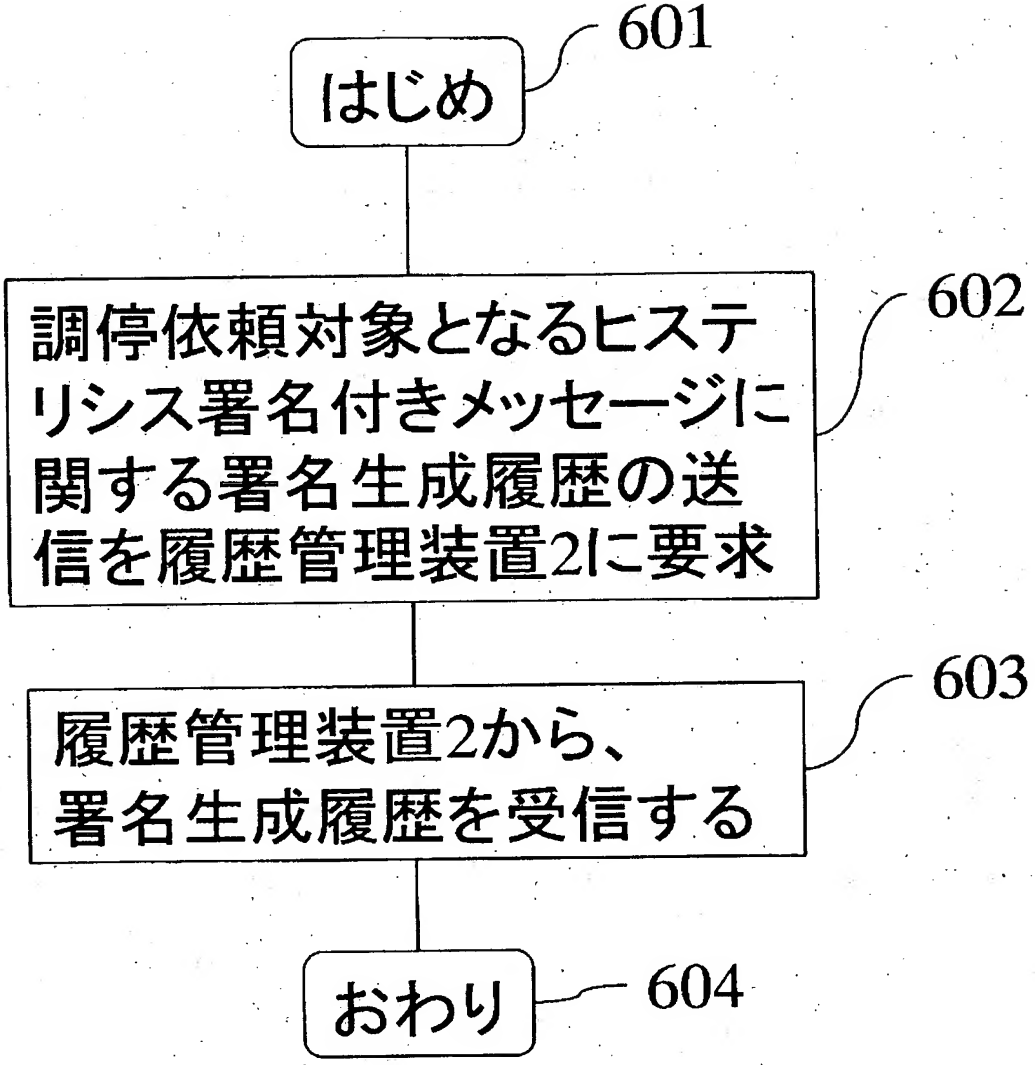
【図５】

図５


501
はじめ
502
履歴送信要求を受け付ける
503
要求を受け付けた範囲の署名生成記録からなる署名生成履歴を要求者に送信する
504
おわり

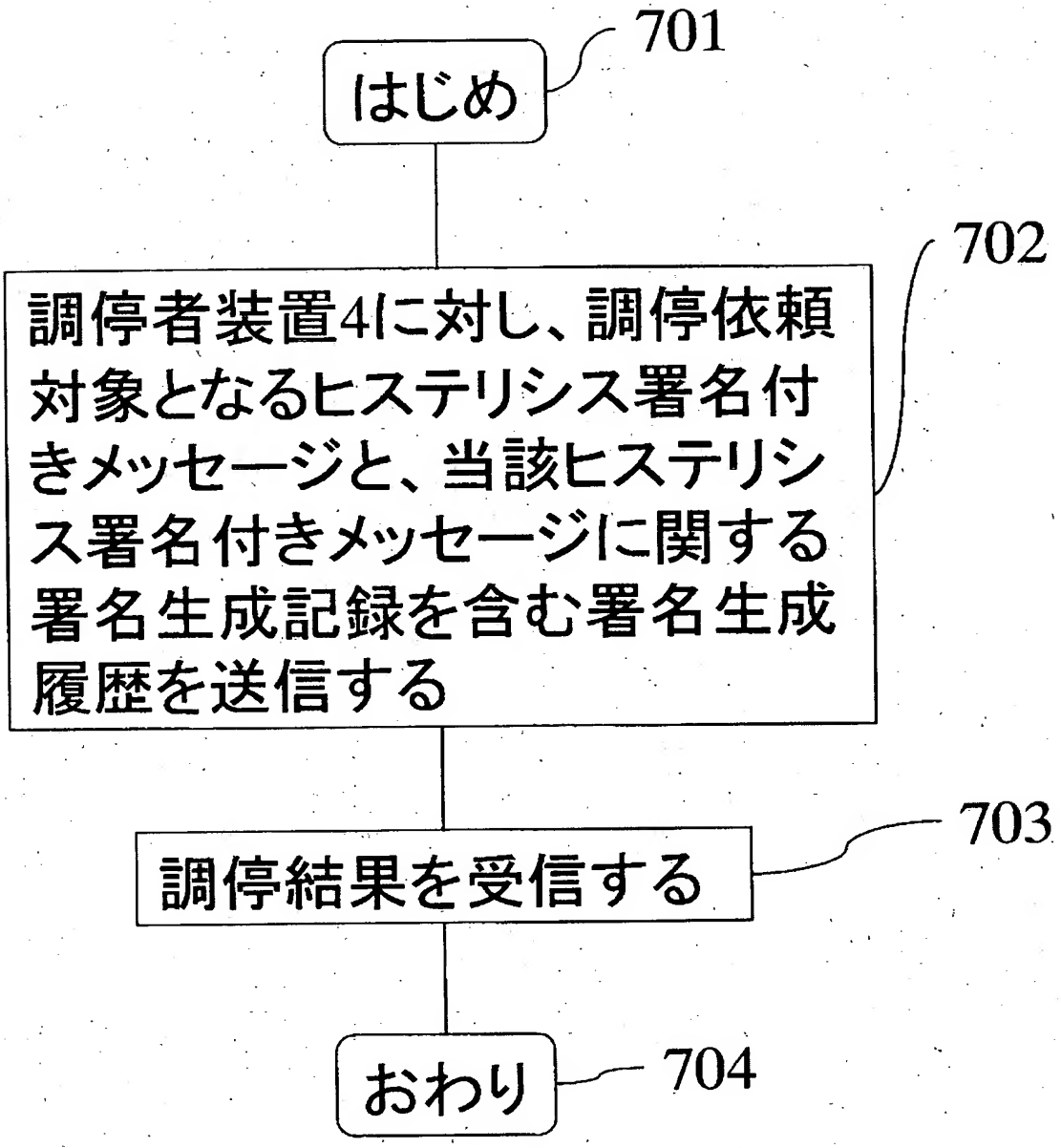
【図６】

図6


はじめ
601
調停依頼対象となるヒステリシス署名付きメッセージに関する署名生成履歴の送信を履歴管理装置2に要求
602
履歴管理装置2から、署名生成履歴を受信する
603
おわり
604

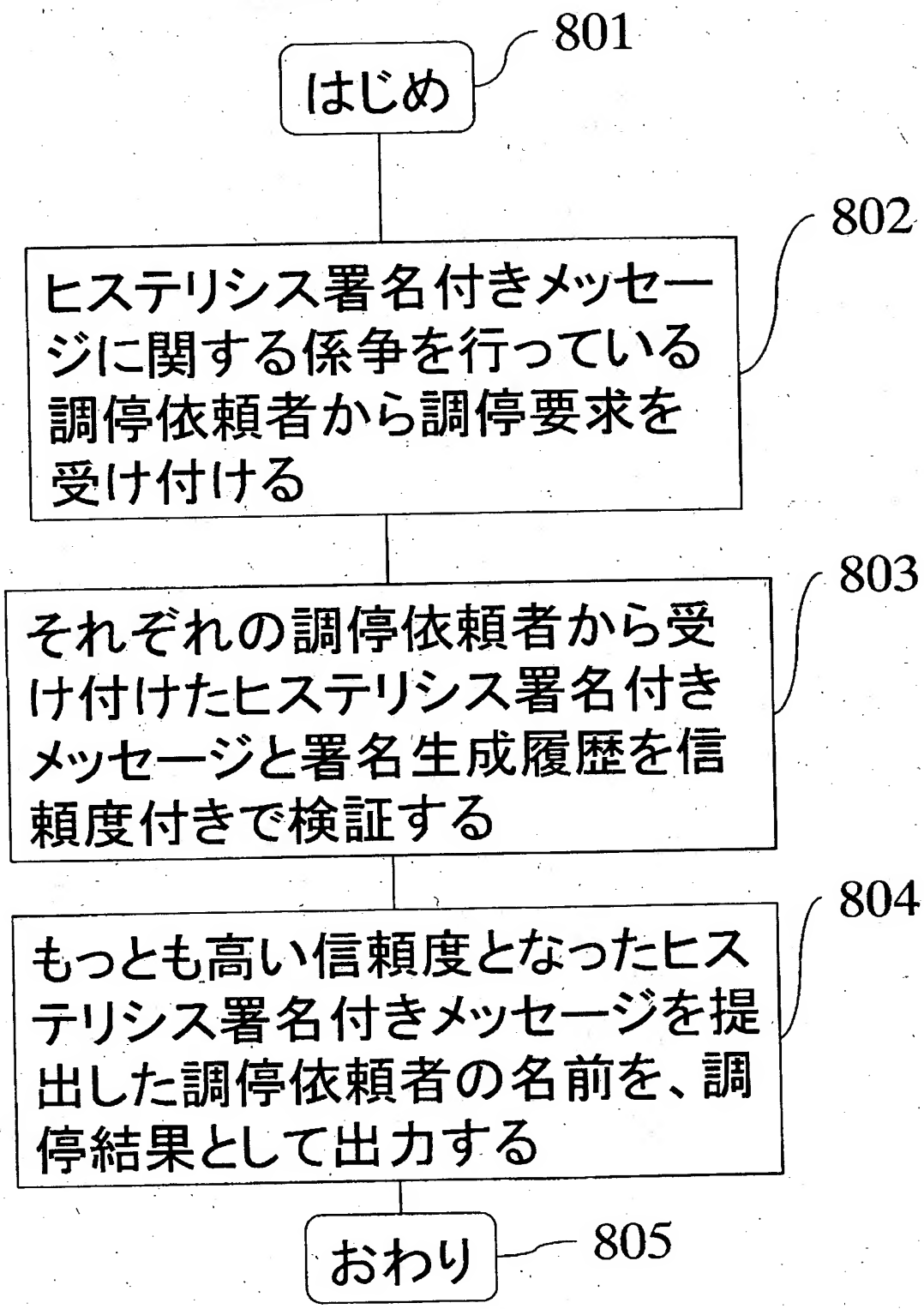
【図７】

図7


701
はじめ
702
調停者装置4に対し、調停依頼対象となるヒステリシス署名付きメッセージと、当該ヒステリシス署名付きメッセージに関する署名生成記録を含む署名生成履歴を送信する
703
調停結果を受信する
704
おわり

【図８】

図8


801
はじめ
802
ヒステリシス署名付きメッセージに関する係争を行っている調停依頼者から調停要求を受け付ける
803
それぞれの調停依頼者から受け付けたヒステリシス署名付きメッセージと署名生成履歴を信頼度付きで検証する
804
もっとも高い信頼度となったヒステリシス署名付きメッセージを提出した調停依頼者の名前を、調停結果として出力する
おわり
805

【書類名】　要約書

【要約】

【課題】

署名履歴に基づいて検証を行うヒステリシス署名において、署名履歴の信頼度を適切に反映するように構成された検証方法と、当該検証方法に基づいて署名の正当性をめぐる係争を解決する調停方法および調停者装置を提供する。

【解決手段】

署名履歴を構成する署名生成記録に信頼度を設定し、設定された信頼度から、署名履歴の信頼度を算出し、算出された信頼度を検証結果の信頼度として出力する。署名履歴の信頼度を適切に反映するように構成された検証方法や、署名の正当性をめぐる係争を解決する調停方法および調停者装置を提供可能となる。

【選択図】　図８

認定・付加情報

特許出願の番号	特願２００２－２０７６９６
受付番号	５０２０１０４４３６８
書類名	特許願
担当官	小野寺　光子　　１７２１
作成日	平成１４年　７月１８日

＜認定情報・付加情報＞

【提出日】　平成14年 7月17日

次頁無

出 願 人 履 歴 情 報

識別番号　〔０００００５１０８〕

１．変更年月日　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所